REMARKS

Claims 1-31 are pending in the application.

The examiner rejected claims 1-28 and 30-31 under 35 U.S.C. §103(a) as being unpatentable over Weiss (U.S. 4,885,778) in view of Kocher (U.S. 6,539,092). Though the examiner appears to believe otherwise, the combination of Weiss and Kocher does not teach or suggest multiple elements of the claimed invention. For example, claim 1 recites:

> generating an authentication code by combining the stored secret, the dynamic value, the first generation value, and the PIN

and also recites:

> generating a second generation value responsive to receipt of the PIN

neither of which features are taught or suggested by Weiss in view of Kocher.

The examiner argues that Weiss discloses generating an authentication code by combining a stored secret, dynamic value and PIN, and he argues that Kocher discloses the first generation value in the form of transaction counter C. However, even if we assume that Weiss and Kocher do disclose these individual elements, the examiner has not pointed to anywhere that Kocher and Weiss teach or suggest combining transaction counter C of Kocher with any other value, e.g., the stored secret, dynamic value, and PIN of Weiss, as required by claim 1. The examiner has also not pointed to anywhere that Weiss and Kocher teach or suggest updating transaction counter C responsive to receipt of a PIN, as required by claim 1. In fact, Weiss in view of Kocher does not teach or suggest either of the above-identified features of claim 1.

Regarding the first mentioned feature of claim 1, "generating an authentication code by combining the stored secret, the dynamic value, the first generation value, and the PIN," the examiner argues that Kocher discloses generating an authentication code by combining transaction counter C, i.e., the claimed first generation value, with a "secret value." Specifically, the examiner argues:

> Kocher thoroughly teaches a security key update process to securely computing, for example, a message authentication code by combining, at least a transaction counter and a secret value (Kocher: Column 4 Line 39-44) (Final Office Action, p. 3).

However, the section of Kocher to which the examiner refers describes using secret key K_C, e.g., the authentication code, but does not describe generating secret key K_C by combining transaction counter C with a "secret value," as the examiner asserts. More specifically, the cited section states:

> At step 110, the device performs the first transaction, using K_C (or a key derived from K_C). The key can be used in virtually any symmetric cryptographic transaction. (For example, such a transaction could involve, without limitation, computing or verifying a MAC (Message Authentication Code) on a message...) (col. 4, lines 39-44).

To summarize, the section describes using secret key K_C for cryptographic transactions. But the intended use of secret key K_C does not provide any information as to whether Kocher actually generates K_C by combining transaction counter C with a "secret value."

In fact, other sections of Kocher indicate that secret key K_C is not generated by combining transaction counter C with a "secret value." Instead, Kocher updates secret key K_C by applying "two forward cryptographic transformations (F_A and F_B) and their inverses (F_A^{-1} and F_B^{-1})" (col. 2, lines 60-61). Kocher describes the process of updating secret key K_C relative to Fig. 1:

> At step 100, the client is initialized or personalized with a starting counter C=0 and a starting state having a starting secret value $K_C=K_0$. At step 110, the device performs the first transaction, using K_C (or a key derived from K_C)...
>
> After step 110, the client device's secret value K_C is updated by applying the function F_A and the counter C is incremented, i.e. by performing $C \leftarrow C+1$ and $K_C \leftarrow F_A(K_C)$. (Thus, at step 111, C=1 and $K_C=F_A(K_0)$.) The updated value of K_C is used to perform a transaction at step 111 (col. 4, lines 37-41 and lines 52-56).

So, before the transaction at step 110, C=0 and $K_C=K_0$. Then, after the transaction at step 110, Kocher increments C, so that C=1, and applies F_A to starting secret value K_0, generating an updated secret K_C. Then K_C is used for a new transaction at step 111. Kocher describes updating secret K_C again after the new transaction:

> After step 111, C is incremented again and F_A is again applied to K_C, i.e. by performing $C \leftarrow C+1$ and $K_{C=2} \leftarrow F_A(K_C)$, yielding the secret key used at step 112 (col. 4, lines 56-59).

In other words, after the transaction at step 111, Kocher increments C, so that C=2, and applies F_A to the previously used secret K_C, generating a newly updated secret K_C. Kocher goes on to describe applying additional functions to K_C after additional transactions.

> The same pair of operations ($C \leftarrow C+1$ and $K_C \leftarrow F_A(K_C)$) are similarly applied between steps 112 and 113, and between steps 113 and 114.
>
> ...After the transaction at step 115, K_C is updated using function F_B by incrementing C and computing $K_{C=6} \leftarrow F_B(K_C)$. After the transaction at step 116, the secret value for transaction 117 is computed by applying the function F_B^{-1} to K_C (col. 4, lines 59-61 and col. 6, lines 1-5).

To summarize, Kocher selects and then applies one of the cryptographic functions F_A, F_B, F_A^{-1}, or F_B^{-1} to secret key K_C. Kocher selects which function to apply based on the value of C: "[t]he choice of which function to apply in any particular state transition can be determined solely as a function of C" (col. 5, lines 33-35). But using the value of transaction counter C to choose and then apply a cryptographic function to K_C is not combining C with a "secret value," or for that matter any value at all.

In fact, if one of skill in the art were to combine the system of Kocher with that of Weiss based on the full teachings of the references, they would at most update Weiss's authentication code by choosing and applying Kocher's cryptographic functions F_A, F_B, F_A^{-1} or F_B^{-1}. But this is not generating an authentication code by combining the transaction counter C of Kocher with a stored secret, dynamic value, and PIN, as required by claim 1.

It may be that the examiner is misconstruing the value K_C as being the product of "K," the secret key, and "C," the transaction counter, and is therefore treating K_C as though it were a combination of K and C. However, Kocher clearly indicates that K_C is the value of secret key K for a particular value of the transaction counter C.

> Each of the boxes in the figure [Fig. 1] represents a value of the secret value (K_C). Thus, multiple dots in a box represent different states sharing the same secret value K_C. The top row (row 0) of the figure contains one box, which corresponds to the initial state K_0 110 as well as subsequent states K_{30} 140 and K_{60} 170, all of which share the same secret value K_C (col. 4, lines 14-20).

In other words, C is simply an index to K. If K_C were the product of K and C, then K_0, K_{30}, and K_{60} would not "share the same secret value K_C," as Kocher discloses, but would instead be

different secret values. Thus, simply writing "K_C" does not mean combining transaction counter C with a "secret value."

The examiner notes that in the Response filed March 14, 2006, we provided example of combining the stored secret, dynamic value, and generation value with an EXCLUSIVE-OR or a one-way function. It appears the examiner believes that we were intending to read these examples into the claims, but that is not the case. We were simply trying to illustrate the plain meaning of the word "combining" recited in claim 1, in order to clarify the ways in which Weiss and Kocher do not teach or suggest combining a second generation value with a dynamic value, first generation value, and PIN.

Regarding the second feature of claim 1 mentioned above, "generating a second generation value responsive to receipt of the PIN," the examiner argues that:

> Kocher is relied upon, besides Weiss, to provide generating a second generation value responsive to receipt of the PIN (Kocher: Column 3 Line 54-60 and Column 4 Line 33-34: a transaction counter is equivalent to a generation value and each transaction counter (including the 2nd generation value) is initiated with a new session of communication requiring the authentication associated with a PIN) (Final Office Action, p. 3).

However, the sections of Kocher to which the examiner refers do not disclose generating a second generation value responsive to receipt of a PIN, but rather simply provide a general description of some of Kocher's variables. More specifically, the cited sections state:

> The client also has a (typically non-secret) index or transaction counter C, which may be initialized to zero. An additional parameter is an index depth D. The value of D may also be non-secret, and (for example) may be client-specific or may be a system-wide global constant. The value of D determines the cycle length of the key update process (col. 3, lines 54-60).
>
> As the states are updated, counter C is also updated (by one for each update) (col. 4, lines 33-34).

Even if we assume that updating transaction counter C is equivalent to a generating a second generation value, these sections do not in any way suggest that it is in response to receipt of a PIN.

In fact, Kocher does not update transaction counter C in response to receipt of a PIN. Instead, Kocher updates C after "transactions" that use secret key K_C, for example:

> computing or verifying a MAC (message authentication code) on a message, encrypting or decrypting a message, producing a pseudo-random challenge, deriving a key, etc.) (col. 4, lines 43-46).

None of these transactions involve a PIN, so Kocher cannot reasonably be construed as teaching or suggesting updating transaction counter C responsive to receipt of a PIN, as the examiner asserts.

Claim 17 is not obvious over Weiss in view of Kocher for similar reasons. For example, the combination of Weiss and Kocher does not teach or suggest:

> a combination subsystem generating an authentication code by retrieving the secret from the memory element and combining the secret and dynamic value from the dynamic value subsystem, the PIN received by the PIN subsystem, and the generation value from the generation value subsystem.

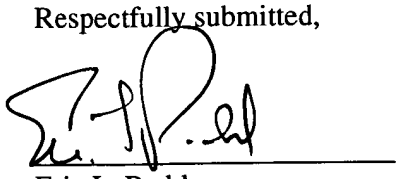
As discussed above, Weiss and Kocher do not teach or suggest methods for combining a secret, dynamic value, PIN, and generation value. Therefore, they also do not teach or suggest a combination subsystem that performs this function. The combination of Weiss and Kocher also does not teach or suggest "calculating a second generation value responsive to receipt of a PIN," as recited in claim 17. The reasons for this are provided above regarding claim 1.

For at least the reasons presented above, applicant believes the pending application is in condition for allowance, and asks the examiner to allow the claims to issue.

No fees are believed to be due at this time. However, please charge any fees, or credit any overpayments, to Deposit Account No. 08-0219.

Respectfully submitted,

Dated: June 12, 2006



Eric L. Prahl
Registration No.: 32,590
Attorney for Applicant(s)

Wilmer Cutler Pickering Hale and Dorr LLP
60 State Street
Boston, Massachusetts 02109
(617) 526-6043 (telephone)
(617) 526-5000 (facsimile)